INT J COMPUT COMMUN, ISSN 1841-9836
8(1):97-104, February, 2013.

Managing Information Technology Security in the Context of Cyber Crime Trends

D. Neghina, E. Scarlat

Diana-Elena Neghina
Institute of Doctoral Studies - ASE
11, Tache Ionescu Street, Bucharest, Romania
E-mail: diananeghina@gmail.com

Emil Scarlat
Academy of Economic Studies
Department of Economic Cybernetics
6, Romana Square, Bucharest, Romania
E-mail: emil_scarlat@csie.ase.ro

Abstract:
Cyber-attacks can significantly hurt an organization's IT environment, leading to serious operational disruptions, from simply damaging the first layers of IT security up to identity theft, data leakage and breaking down networks. Moreover, the dangers through which current cybercrimes practices affect organizations present a tendency of developing more rapidly that decision makers can assess them and find countermeasures. Because cyber threats are somewhat new thus a critical source of risks, within the context of the constantly changing IT environments (e.g. cloud services integration) organizations may not effectively implement and manage cyber threat risk assessment processes. This paper highlights the importance of designing effective security strategies and proactively addressing cybercrime issues as key elements within the organizational risk management approaches.
Malware rises constantly in impact and complexity and has surpassed the traditional security model. One of the main ideas of the study is to present the main areas of risks related to cyber security to which an organization is subject to and provide a baseline of an analysis model that would adequately evaluate input data, rank priorities and represent the results and solutions to decrease these risks. The importance of this study is to increase awareness efforts and to highlight the critical importance of using the full extent of resources provided. Each member of an organization has a significant role in decreasing the exposure to the vulnerabilities created by cyber-attacks.
Keywords: Cybercrime, IT security, risk assessment, vulnerability management.

1 Introduction

The dangers through which current cybercrimes practices affect organizations present a tendency of developing more rapidly that decision makers can assess them and find countermeasures, exposing entities to significant risks. Vulnerability events are created constantly, through the exposure over shared environments(such as cloud solutions), permanent transfers of critical information between an organizations branches, social platforms, electronic banking solutions, displaying intellectual property, all enabling favorable circumstances for appropriation, disturbances and misuse of critical information and data.

The purpose of this paper is to make entities aware of the changes in the last decades of cyber threats within network environments and how to effectively approach these elements, timely finding solutions and actions to be taken. One of the main ideas of the study is to present the principal areas of risk related to cyber security to which an organization is subject to in the current IT environments and to determine a specific analysis model that would adequately lead

to input data evaluations, rank priorities and represent the results and solutions to mitigate the identified risks.

On the current market, the tendency of decision makers is still to take unintended or unexpected risks by following classical patterns of behavior and standard models of security, applied additionally in new environments that are continuously changing, often with the consequence of significantly affecting organizational value.

Our opinion is that the increasing number of attacks and constantly developing threats are leading to significant gains that are further supporting the constant adaptation of cyber criminals to the classical implementation and management of security tools. We consider that our paper is raising an alarm signal on the lack of perception of the fact that traditional models are starting to be considered as outdated and decision makers must evaluate the need of combining them with additional elements from the operational areas to obtain a better understanding; the real issue is the fact that professional cybercrime tools and methods are so advanced that are continuously increasing the security issue.

Managements ability of forecasting security breaches that are considered critical for the compliance of a company with its strategies is essential in using corporate information as an asset, as well as a significant competitive advantage. This further sustains the capability of a close collaboration between IT resources and operational ones. Technical understanding of events and processes must be combined with the business perception of processes and activities for entities to adjust more quickly to challenges and take immediate actions to unexpected events.

Even though IT governance and compliance methods, identity management, applications security and network tools are becoming more and more complex, are processing information from different areas of an organizational environment, cyber criminals are also aware of the changes and are also adjusting their techniques, becoming better at hiding their trace, gaining undetected access and all for extended durations of time; studies present the fact that they are characterized by stealthy and passive methods for attacking a system (Schudel, Wood) [1].

Entities must better determine the key elements that are making them a target of cyber criminals and the way they are perceived by external parties regarding critical information of interest and act on these vulnerabilities first, these being considered as the initial layers of attack.

All security analysis and prevention methods should begin from the idea of unauthorized access being gained and core business data being misused, thus leading to appropriate security measures of classification of critical information (high to low risk assessments). As a general overview of IT reviews, there are not many entities that are implementing levels of security and classification of data based on values or risk considerations.

As a summary conclusion, the actual warning is the tendency of cybercrime attacks of continuously becoming more dangerous and complex, evolving into schemes difficult to anticipate. The attacks are determined to be more destructive, more advanced and more studied (significant resources are invested in these activities, new capabilities are researched based on existing security tools) and have a serious impact over economic and even national security elements.

2 Cyber-Crime Trends Analysis

The current approaches of cyber criminals may be characterized as proactive. Further, attackers actions are dynamic through their frequency and most aggravating, collaborative, in the sense that services emerge over the Internet with the scope of committing fraud, theft and exploitation of systems vulnerabilities.

2.1 Brief development of cyber crime

As a summary of cyber-attacks tendencies, during the first periods of modern Internet and IT environments, cyber-attacks were generally performed by employees, within organizational networks, generally due to different dissatisfaction reasons. This type of threat was favored until the 1980 and attackers took advantage of privileged and granted access privileges to IT resources; they altered information mainly for financial advantages or simply sabotaged data for revenge at employers.

Studies revealed that programmers developed their abilities of writing malicious software, including self-replicating programs, to interfere with personal computers. During the 1990s, financial crime over the Internet completed through penetration and subversion of computer systems increased significantly. By the late 1990s and in the years following 2000, fraud attacks and identity theft developed. Moreover, organized attacks started to be performed more often including groups of cyber criminals and increasing the time of acting out without any detection (Kabay) [3].

Throughout the 2000s, cyber attackers started to externalize services and offer their unauthorized activities for more complex crimes. There were identified many denial-of-services attacks opposing known websites and malware was designed to record logs of keystrokes and then send this information through secure Internet communication channels to cyber criminals.

2.2 Trends and security challenges

Thus, business data, organizational assets are increasingly threatened and traditional IT security approaches are offering only the basis of solutions. As a general characteristic, the present IT environment can be considered as reactive, without any time allocated for risks assessments; cyber criminals are aware of all these exposures and take advantage of them through the use of end users (social engineering, theft of credentials), phishing attacks, through all sorts of original deceptions, penetration and encryption techniques to make their trace inaccessible.

As mentioned previously, security events are continuously increasing, in frequency as well as in impact. However, in the same time quantitative information related to these events are both difficult to obtain as well as hard to place into a meaningful framework (Shimeall, Williams) [2].

On a general level, organizations should transition from a mainly security based approach to a more risk assessment approach, thus addressing vulnerabilities within the risk management planning and methods. Entities should continuously increase their security awareness procedures, apply active monitoring procedures and complete periodical trainings for all operational and technical personnel to achieve an effective cyber security stance.

Operational and information technology solutions are shifting towards collaboration environments. IT environments sustain shared resources and services, including core business applications, centralized architecture and infrastructure elements for which entities must put in place controls to identify and counteract effectively unauthorized actions. Thus there must be put in place techniques that set the baseline for risk control and business efficiency, outlining the key issues and introducing risk assessments of specific elements regarding enterprise information protection and personal privacy.

However, the vast majority of organizations have restricted abilities to identify and take effective actions against security breaches. Researches show that preventive actions are extremely hard to implement. Moreover, most of the current analysis tools are based on prior behavior and activities and may not produce significant models to appropriately identify other attacks or to be used for efficient preventive actions (Jajodia et al) [4]. Vulnerabilities are thus analyzed constantly based on prior security events and not on emerging cyber threats, adding value to the security outline of the organization.

However, in practice, defined security assessments performed by organizations are not capable any more to cope with the continuously evolving threats. These are not focused on collecting cyber threat data from a variety of business and operational areas and different sources due to increased time allocation and costs of implied resources. Security methods applied are based mainly on high level information and tools and technologies implemented are generally configured based on existing standards, and not customized on the features of the environments that would have the ability to promptly identify, enclose and restrict, evaluate and restore compromised characteristics.

With the difficulty of obtaining and updating cyber intelligence information, the implementation of risk management methodologies should be performed. These must be appropriately designed and used to effectively challenge or even block access attempts, security breaches or fraudulent transactions. In the following section we present the approach distinguished through a set of specific tools and techniques that can be easily customized and applied to specific organizations profiles, networks, and significantly improve the already implemented security controls by organizations.

3 Cyber Threats Risk Management Capability

The risks characteristic for an organization and its related industry shape the operational environment, its readiness and effective response to different interactions with internal and external environments. The general characteristic of the current organization is its increasing reliance on technology, information sharing, and connectivity elements. Thus dependence leads to risks at all levels.

Due to the fact that cyber threats are a relatively new and constant source of risk, continuously changing, entities are not as capable at managing cyber threat risk as they are at managing any other operational risk related to business activities.

3.1 The fundamentals of a cyber-threat risk assessment process

Unless an organization is considerably developed related to cyber threat risk management practices, it cannot have the risk assessment infrastructure and governance elements designed to sustain an adequate security environment. For example, if the basic elements are not defined, such as specific risk definitions and business impact analysis, risk limits of acceptance or specific key performance indicators.

If an enterprise cannot sustain at least the above mentioned elements, it is advisable as a starting point the evaluation of the following set of information security practices that significant for an appropriate cyber risk assessment process:

1. Existing security controls, implemented by the entity to identify and record known types of cyber-attacks that are characterized by stealth breaches. Here are included also the security tools and techniques used to timely identify and contain compromised IT resources;

2. Available methods of recording security breaches information from multiple sources (internal as well as external). Added to this category are the abilities of the entity to implement cyber-crimes risk models in order to collect relevant cyber intelligence information and generate value and actionable data for decision making purposes;

3. Exposure of employees to complex social engineering attacks that allows malware to be integrated in the administrative consoles or workstations. Here are included the procedures of detecting advanced, persistent threats within the entitys own business environments in the case of identity theft or unauthorized use of authentication elements.

These are not topics for an elaborate analysis process, but they do represent basic elements of an effective defense mechanism against current cyber-attacks. By applying a more elaborate cyber threat risk assessment framework (presented in Figure 1. and further detailed in the following section) an organization can better protect its operational environments as well as gain valuable insights on its vulnerabilities and improvement actions to be taken.

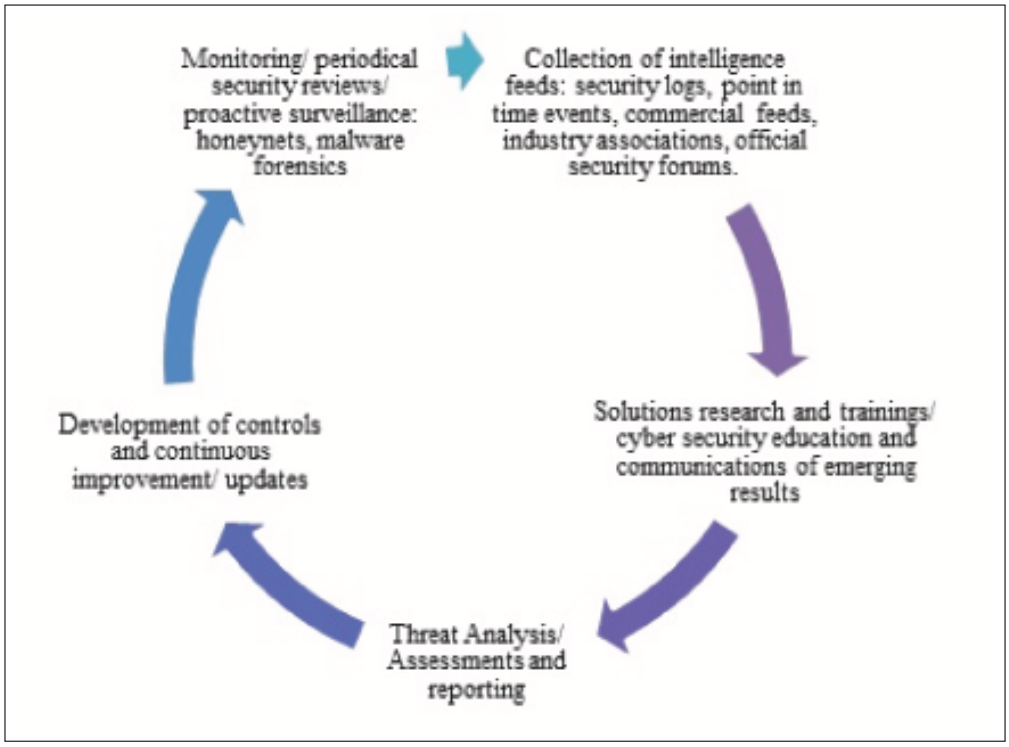

Figure 1: Model score **after** boosting

3.2 Core cyber threats risk management capabilities

Below we present a new approach of cyber threat risks that, if unaddressed, may lead to the security vulnerabilities exploited firstly by attackers.

1. Monitoring and key performance indicators:

Starting from the basic incident driven communication with management, periodical and formalized communication with decision makers should be implemented. Evidence should be kept for ongoing dialogue and critical metrics should be reviewed, analyzed and used to improve already existing security controls.

Key performance indicators should be designed based on cyber intelligence information that must be logged for predefined periods of time. These must be standardized within the organizational units and have a clear linkage to business value (generally these should be defined in quantitative terms).

2. Organizational personnel:

Employees must be aware of cyber threat risk, recognize attacks as a potential risk area and have basic knowledge of designed security policies, processes, and implemented tools; roles and responsibilities for risk management should be established that would ensure the integration of specific risk assessments into larger security decisions and controls affecting an organization.

IT personnel must have specialized knowledge about cyber threat risk; moreover, as a required competency security feeds from operational units must be centrally coordinated to manage and

keep cyber threat risks within defined acceptance levels.

Written and approved IT security policies, training missions, and communications must be effectively distributed and compliance periodically monitored and reviewed for appropriate enforcement; most of employees should have clearly defined responsibilities for cyber risk management, appropriate to their roles and responsibilities.

3. Operational processes:

Organizational business units are characterized by fragmented processes, which are not always communicating between them, certain manual input and execution of operational activities. Defined processes must align with enterprise-wide risk management framework above mentioned and must be monitored by IT personnel and executive management at different levels; processes must reach the level of being consistently integrated, automated, and clearly documented related to cyber threats risk assessments.

Organizations must formally measure and monitor process effectiveness; automation must be viewed as an objective; cyber threat risk management may be organized at a higher level as a self-standing unit and through which all processes are addressed by continuous improvement efforts; the overall objective is to accomplish structured cyber threat risk management programs that are integrated with the already existing IT risk management and enterprise risk management agendas.

4. Security tools and techniques:

Technology already installed for security reasons must be enabled to log security events, to centralize them and as a basis must send alerts in case of incidents recorded or exceptions; signature-based controls such as anti-virus and intrusion-detection software must be implemented. For an evolved organizational environment, forensic tools may be used for reacting to exceptional security events.

Commercially available threat monitoring feeds may be integrated with centralized logging solutions and monitoring software to generate automated alerts. For more complex risk management existing security tools may be automatically enabled to perform advanced correlations related to threat information and to convert obtained data into actionable alerts. These methods applied may be used to automate not just threat monitoring and alerts, but further security events identified, such as malware, or complete forensic analysis, as well as more complex threat assessments.

The presented framework of continuously evolving cyber threat risk management capability model may sustain an organization in the process of implementing better security techniques to avoid cyber-attacks of criminals that make it past the already existing access controls mechanisms.

For example, a well-developed cyber threat risk management model will include safety elements against unauthorized information distribution, as well as protection opposed to unauthorized information access. Effective completion of these features lead to the use of technologies and processes that monitor outbound information traffic for both content and destination in particular. This can be configured as an alert point if data is being transferred to a location outside the normal operational environment, where the organization has not been present before. An accomplished capability will also be able to contain the transfer of information timely, to isolate the elements involved and assess the suspicious communication networks until their authentication credentials are clear; in case of unauthorized actions, procedures are in place for forensic analysis.

Because cyber-attackers are continuously improving their identity theft techniques, an organization shouldnt assume that each user that authenticates at network level and within the IT application systems and is performing the required activities with legitimate credentials is in reality a legitimate user, an employee or an agreed service provider of the entity.

A complex cyber threat risk management process will be designed to use at least two verification methods, depending on the classification of the information being protected. These activities include the verifications of a persons physical identity through techniques including biometrics such as laptop fingerprint readers, PIN code token devices that must be carried by the legitimate users at all times, and finally behavioral programs that track post-login activity against historical patterns defined for a specific user in order to determine the likelihood of that person authenticating of being legitimate.

4 Discussions

Any cyber-attack can hurt an organization in any number of ways, ranging from minor damages to a website informative page to shutting down core networks, committing fraud, and stealing intellectual property. Thus organizations should implement actionable, risk-based intelligence processes in order to timely identify unauthorized cyber activity. Entities should maximize the use of existing security solutions, logged information and most important, completing cyber threat awareness programs among employees. As a summary process, an organization should effectively identify the cyber-criminal risk, assess and evaluate this risk, integrate it, respond and take isolation actions to the risk, design, implement and test appropriate security controls, further monitor events, as well as assure and escalate future cyber-attacks.

As mentioned within prior studies, cyber-crime events will become more precise, more specialized, and for this reason organizations must integrate a dedicated cyber threat analysis tools and IT experts. As a general idea, an organization's security resources will need to focus more on analyzing available internal and external data sources, customize controls and center less on managing and maintaining standard security controls.

5 Conclusions

Entities are responsible for implementing and maintaining an integrated approach between its employees, operational process, and technology resources implemented in order to complete effective risk management procedures. Resources must be allocated to gather and process cyber threat analysis information, notifying the results and defining alerts for better security controls and measures to be taken by the operational units.

Complex cyber risk management processes are repeatable, clearly defined, well-documented, and aligned with an organizations larger IT risk management. Future work will focus upon cyber intelligence collection methods and processing algorithms, behavioral trends of cyber attackers, which could accommodate customized improvements to the risk management activity of an organization. As the research of cyber security capabilities transforming from raw data to actionable intelligence will provide valuable cyber threat research. Hence, such an analysis would support improvements in multiple key threat indicators and metrics related to IT security analysis.

Bibliography

[1] Gregg Schudel, Bradley Wood, *Modeling Behavior of the Cyber-Terrorist*, in $http://www.dli.gov.in/data/HACKING\_INFORMATION/PRINTED20PAPERS/Modeling20Behavior20of20cyber20terrorist.pdf$.

[2] Tim Shimeall, Phil Williams, *Models of Information Security Trend Analysis*, in $http://www.dli.gov.in/data/HACKING\_INFORMATION/PRINTED20PAPERS/models20for20inf20security20TREND20ANALYSIS.pdf$.

[3] M. E. Kabay, *MA Brief History of Computer Crime*, in http://www.mekabay.com/overviews/history.pdf.

[4] Sushil Jajodia, Peng Liu, Vipin Swarup, Cliff Wang, Editors, *Cyber situational awareness: Issues and Research*, in Springer International Series on ADVANCES IN INFORMATION SECURITY.

[5] Sumit Ghosh, Elliot Turrini, Editors, *Cybercrimes: A Multidisciplinary Analysis*, in Springer-Verlag Berlin Heidelberg, 2010.

[6] Martin C. Libicki, *Cyberdeterrance and Cyberwar*, Rand Corporation, 2009.

[7] Jean-Marc Seigneur, Adam Slagell, *Collaborative Computer Security and Trust Management*, in Information Science Reference (an imprint of IGI Global), 2010.